(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 051 011 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
08.11.2000 Bulletin 2000/45

(51) Int Cl.[7]: **H04L 29/06**, H04L 12/22

(21) Application number: **99307199.2**

(22) Date of filing: **13.09.1999**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **01.05.1999 KR 9915770**
01.05.1999 KR 9915771

(71) Applicant: **Samsung Electronics Co., Ltd.**
Suwon-city, Kyungki-do (KR)

(72) Inventors:
- **Lee, Chang Hyi, Apkujung Building**
  Seoul (KR)
- **Chung, Ho Suk**
  Kangnam-gu, Seoul (KR)
- **Kang, Eun-Seong**
  Kangnam-gu, Seoul (KR)

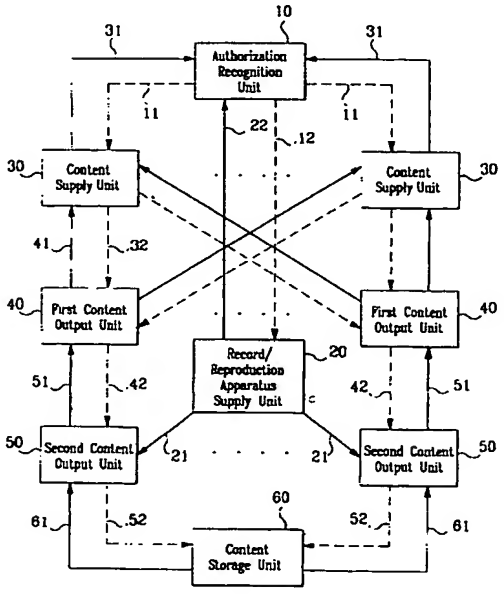
(74) Representative: **Chugg, David John et al**
Appleyard Lees,
15 Clare Road
Halifax, West Yorkshire HX1 2HY (GB)

(54) System for preventing an illegal copy of digital contents

(57) In order to prevent an illegal copy of an encoded digital content downloaded by users for reproduction, all systems connected to the users generate a plurality of keys which are mutually shared, and download and upload the digital content by using channels formed between units performing mutual communication

A unit for supplying the digital content receives an authorization of legally supplying the digital content from an authorization recognition unit. A first content output unit (40) is authenticated form a digital content supplying unit (30). At this time, the digital content supplying unit (30) and the first content output unit (40) form a sharing key to form a channel between the two. A second content output unit (50) is authenticated from the digital content supply unit (30) through the first content output unit (40), the first content output unit (40) and the second content output unit (50) form a channel to the channel key. The digital content between the first content output unit (40) and the second output unit (50) is downloaded and uploaded according to respective control state data of the first content output unit (40) and the second output unit (50). Accordingly, the digital content transmitted between the digital content supply unit (30), the first content output unit (40), and the second content output unit (50) can be prevented from an illegal copy.

FIG.1



EP 1 051 011 A2

Description

[0001] The present invention relates to a system for preventing an illegal copy of digital contents, and more particularly to a system for preventing an illegal copy of digital contents which forms secret channels between all the systems connected to users and exchanges contents through the formed secret channels in order to safeguard digital contents from illegal copying.

[0002] In recent years, the communications environment has rapidly been developed when considering that a lot of data is provided through the internet, a lot of terminal units are provided to which data can be easily downloaded from the internet through internet hookup, and the like.

[0003] Therefore, people obtain a wide variety of data by using such a communications environment. That is, individuals have internet appliances having communication equipments and download various data from the internet by using the internet appliances.

[0004] The term internet appliance is intended to cover equipment such as a PC phone, a PDA, a Web Phone, a Mobile Phone, and the like, which are hereinafter referred to herein as first content output units in.

[0005] Because of the expansion in the communications environment, there are now many digital content suppliers who are willing and able to provide much more digital data to such first content output units than previously, and those digital contents suppliers provide users with digital contents to such first content output unit, by compressing the contents according to MP3, AAC, G2 methods.

[0006] Digital contents which are used in the present invention mean all data including audio, video data, as well as character data such as song words, movie captions, and the like to be provided through the internet.

[0007] In particular, the MP3 which is the audio data of the above digital contents is downloaded to the first content output unit as well as the second content output unit such as an MP3 player and then reproduced.

[0008] In the meantime, the MP3 is downloaded to a content storage unit such as a smartmedia card built in the first content output unit, and the MP3 downloaded in the content storage unit is reproduced through the second content output unit.

[0009] However, as stated above, there is a drawback in that digital data downloaded to the first and second content output units and the content storage unit is easily copied to be illegally distributed.

[0010] With a view to solve or reduce the above problem, it is an aim of embodiments of the present invention to provide a system for preventing an illegal copy of digital contents for preventing the illegal copying and distribution of digital content downloaded by forming a secret channel between all the system mutually connected as users download and reproduce the digital content.

[0011] According to an aspect of the present invention, there is included an authorization recognition unit for generating a first authentication qualification key and a first authentication qualification key data in response to a second, externally input, registration request signal, a content supply unit for transmitting the second registration request signal to the authorization recognition unit, storing a first authentication qualification key and the first authentication qualification key data inputted from the authorization recognition unit, and generating a second authentication qualification key and a second authentication qualification key data, and a first content output unit for outputting the third registration request signal to the content supply unit, and storing the second authentication qualification key and the second authentication qualification key data inputted from the content supply unit.

[0012] Preferably, the authorization recognition means forms a first channel key capable of sharing with the content supply means in response to a first registration request signal inputted from the content supply means, and outputs an encoded first authentication qualification key and an encoded first authentication qualification key data to the content supply means via a secret channel formed by the first channel key.

[0013] The content supply means may interpret and store the first authentication qualification key and the first authentication qualification key data input from the authorization recognition means via the secret channel by using the first channel key.

[0014] The content supply means may form a second channel key capable of sharing with the first content output means in response to the second registration request signal input from the first content output means, and output a second authentication qualification key and an encoded authentication qualification key data to the first content output means through a secret channel formed by the second channel key.

[0015] Preferably, the first content output means interprets and stores the second authentication qualification key and the second authentication qualification key data inputted from the content supply means through the secret channel by using the second channel key.

[0016] According to a second aspect of the invention, there is provided a system for preventing an illegal copy of digital contents, comprising: authorization recognition means for generating a manufacturer key and a manufacturer key data in response to an externally input first registration request signal, generating a first table and a second table by using the manufacturer key and the manufacturer key data, and generating a first authentication qualification key and a first authentication qualification key data in response to the second registration request signal inputted from external; record/reproduction apparatus supply means for outputting the first registration request signal to the authorization recognition means, and storing the manufacturer key and the manufacturer key data inputted from the authorization recognition means; content supply means for outputting the second registration request signal to the authorization

recognition means, storing the first authentication qualification key, the first authentication qualification key data, and the second table, and generating a second authentication qualification key and a second authentication qualification key data in response to an externally input third registration request signal; first content output means for outputting the third registration request signal to the content supply means, storing the second authentication qualification key and the second authentication qualification key data input from the content supply means, outputting the externally input manufacturer key data to the content supply means, encoding and outputting the manufacturer key detected from the second table in response to the manufacturer key data; and second content output means for storing the manufacturer key and the manufacturer key data input from the authorization recognition means, outputting the manufacturer key data to the content supply means through the first content output means, and comparing the manufacturer key with the manufacturer key of the second table input from the first content output means in order to judge if the stored manufacturer key is authenticated.

[0017] Preferably, the first table generated from the authorization recognition means contains the manufacturer key data, the manufacturer key, and an identifier corresponding to the manufacturer key, and is stored only in the authorization recognition means.

[0018] The second table generated from the authorization recognition means and output to the content supply means has an identifier corresponding to the manufacturer key data and the manufacturer key, data from encryption of the manufacturer key by using a token, and a token.

[0019] A content storage means may be further included which is connected to the first content output means or the second content output means and stores data downloaded from the content supply means.

[0020] Preferably, the authorization recognition means forms a first channel key capable of sharing with the content supply means in response to a first registration request signal inputted from the content supply means, and outputs an encoded first authentication qualification key and an encoded first authentication qualification key data to the content supply means via a secret channel formed the first channel key.

[0021] The content supply means preferably forms a second channel key capable of sharing with the first content output means in response to the second registration request signal input from the first content output means, and outputs a second authentication qualification key and an encoded authentication qualification key data to the first content output means through a secret channel formed by the second channel key.

[0022] Preferably, the first content output means interprets and stores the second authentication qualification key and the second authentication qualification key data inputted from the content supply means through the secret channel by using the second channel key.

[0023] The token may be randomly generated by the authorization recognition means.

[0024] The first content output means preerably forms a third channel capable of being shared with the second content output means, encodes the third channel key with a token inputted from the content supply means and transmits to the second content output means.

[0025] The second content output means may extract a token from encoded manufacturer data from the first content output means by using the stored manufacturer key in advance, interprets and stores the third channel key by using the token to form a secret channel with the first content output means.

[0026] According to another aspect, there is provided a system for preventing an illegal copy of digital contents, comprising: content supply means for supplying an encoded digital content; first content output means including a database which has reproduction data of a digital content downloaded from the content supply means, encoding the database by using the third channel key for storage, interpreting the reproduction data of the digital content inputted from external by using the third channel key to be compared with a reproduction data of the database, to thereby judge if an illegal copy of the digital content is performed; and second content output means for updating the reproduction data of the digital content stored in advance by interpreting the reproduction data of the digital content input from the first content output means by using the third channel key, and transmitting the updated reproduction data of the digital content to the first content output means.

[0027] The database may be separated with an identifier data area of the digital content, an updated token data area, an data area for a present state of the digital content, and a reproduction control data area, and has the corresponding data.

[0028] The data area for the present state of the digital content preferably include: data indicating that the digital content is downloaded in a copy form from the first content output means to the second content output means; data indicating that the digital content is downloaded in a transmission form from the first content output means to the second content output means; and data indicating that the digital content is downloaded and uploaded between the first content output means and the second content output means.

[0029] The reproduction control data area of the digital content may include: data for reproduction times of the digital content; data for a reproduction expiration period of the digital content; and data for an amnesty period of the digital content.

[0030] For a better understanding of the invention, and to show how embodiments of the same may be carried into effect, reference will now be made, by way of example, to the accompanying diagrammatic drawings in which:

Figure 1 is a schematic view for explaining a system

for preventing an illegal copy of digital contents according to an embodiment of the present invention;

Figures 2-5 are views for briefly explaining registration requests or digital content reproductions of respective blocks of Figure 1;

Figure 6 is a view for showing an example of a file format which is supported by the embodiment of the present invention;

Figure 7 is a block diagram for showing digital content processes in a content storage unit of the embodiment of the present invention;

Figure 8 is a view for showing an output source capable of being additionally connected to the embodiment of the present invention; and

Figure 9 is a view for showing an input control block diagram for supporting the output source of Figure 8.

[0031] Hereinafter, an preferred embodiment of the present invention will be described in detail with reference to the accompanying drawings.

[0032] Figure 1 is a schematic view for explaining a system for preventing an illegal copy of digital contents according to an embodiment of the present invention, in which the structure is as follows.

[0033] An authorization recognition unit 10 generates a manufacturer key and a manufacturer key data 12 in accordance with a first registration request signal 22 inputted from a record/reproduction apparatus supply unit 20, described later, and outputs a manufacturer key and a manufacturer key data 12 to the record/reproduction apparatus supply unit 20. Further, the authorization recognition unit 10 uses the manufacturer key and a manufacturer key data 12,generates first and second tables , and generates a first authentication qualification key and a first authentication qualification key data 11 in accordance with a second registration request signal 31 inputted from a content supply unit 30.

[0034] The first authentication qualification key and the first authentication qualification key data 11 mean a public key ($PubKey_{ISP}$), a public key data($Cert_{CA}(PubKey_{ISP})$), and a private key($PrvKey_{ISP}$) of the content supply unit 30 generated from the authorization recognition unit 10.

[0035] Further, the first table, as shown in Figure 2, contains a manufacturer key data($Cert(MK_{PD})$), the manufacturer key(MK_{PD}), and an identifier(ID_{MK}) corresponding to the manufacturer key data and the manufacturer key, and is stored in only the authorization recognition unit 10. Further, the second table is generated from the authorization recognition unit 10 and outputted to the content supply unit 30, and contains the identifier (ID_{MK}), data($ENC(MK_{PD}, T)$), and a token(T) which encodes the manufacturer key by using the token.

[0036] At this time, the authorization recognition unit 10 forms a first channel key(k) which can be shared with the content supply unit 30 in accordance with the second registration request signal 31 inputted from the content supply unit 30, and outputs the first authentication qualification key and the first authentication qualification key data 11 which is encoded into the content supply unit 30 through a secret channel formed by the first channel key (k).

[0037] The first channel key is a key generated from encryption of the authorization recognition unit 10 by using data which the content supply unit 30 has.

[0038] The record/reproduction apparatus supply unit 20 outputs the first registration request signal 22 to the authorization recognition unit 10, stores and manufactures the manufacturer key and the manufacturer key data(MK_{PD}, ($Cert_{CA}(MK_{PD})$; 12) inputted from the authorization recognition unit 10 to be recorded in internal memory of the second content output unit 50, described later, which is a record/reproduction apparatus.

[0039] The content supply unit 30 outputs the second registration request signal 31, stores the first authentication qualification key, the first authentication qualification key data, and the second table 11 inputted from the authorization recognition unit 10, and generates a second authentication qualification key and authentication qualification key data 32 in response to a third registration request signal 41 inputted from the first content output unit 40 described later.

[0040] In the meantime, the content supply unit 30 interprets and stores the first authentication qualification key and the first authentication qualification key data 11 inputted from the authorization recognition unit 10 through the secret channel by using the first channel key k.

[0041] At this time, the content supply unit 30 forms the second channel key k which can be shared with the first content output unit 40 in response to the second registration request signal 41 inputted from the first content output unit 40, and transmits the second authentication qualification key($PubKey_{ISP}$) and the second authentication qualification key data($Cert_{CA}(PubKey_{ISP})$) which are encoded as the first content output unit 40 through the secret channel formed by the second channel key(k).

[0042] The first content output unit 40 outputs the third registration request signal 41 to the content supply unit 30, stores the second authentication qualification key and the second authentication qualification key data 32 inputted from the content supply unit 30, transmits a manufacturer key data inputted from the second content output unit 50, described later, to the content supply unit 30, encodes and outputs the manufacturer key detected from the second table in response to the manufacturer key data.

[0043] The second channel key(k) is a key generated through encryption of the content supply unit 30 by using

data which the first content output unit 40 has, and is shared by the content supply unit 30 and the first content output unit 40.

[0044] Further, the first content output unit 40 stores a database encoded by the third channel key (CK_{PD-LCM}), wherein the database has a digital content reproduction data downloaded from the content supply unit 30, interprets by the third channel key(CK_{PD-LCM}) the digital content reproduction data inputted from the second content output unit 50, and compares the digital content reproduction data with the database production data, and judges whether the digital content has been illegally copied.

[0045] Here, the database contains an identifier data area of the digital content, an updated token data area, a data area for a present state of the digital content, and a reproduction control data area.

[0046] Further, the data area for a present state of the digital content has data informing if the digital content is downloaded from the first content output unit 40 to the second content output unit 50 in a copy form, data informing if the digital content is downloaded from the first content output unit 40 to the second content output unit 50 in a transmission form, and data informing if the digital content is downloaded or uploaded between the first content output unit and the second content output unit.

[0047] Further, the reproduction control data area of the digital content has data for reproduction times of the digital content; and data for reproduction expiration period of the digital content, and data for amnesty period of the digital content.

[0048] In the meantime, the first content output unit 40 interprets and stores the second authentication qualification key and the second authentication qualification key data inputted from the content supply unit 30 through the secret channel by using the second channel key(k).

[0049] Lastly, the first content output unit 40 forms the third channel key(CK_{PD-LCM}) which can be shared with the second content output unit 50, encodes the third channel key(CK_{PD-LCM}) inputted from the content supply unit 30 into a token, and transmits the second output unit 50.

[0050] At this time, the token T is randomly generated by the authorization recognition unit 10.

[0051] The second content output unit 50 stores the manufacturer key(MK_{PD}) and the manufacturer key data ($Cert_{CA}(MK_{PD})$) inputted from the authorization recognition unit 10, transmits the manufacturer key data to the content supply unit 30 through the first content output unit 40, and compares the manufacturer key with the manufacturer key of the second table inputted from the first content output unit 40 for judging if the stored manufacturer key is authenticated.

[0052] Further, the second content output unit 50 extracts a token from the manufacturer key data encoded in the first content output unit 40 by using the stored manufacturer key, and interprets and stores the third channel key(CK_{PD-LCM}) by using the token to form a secret channel with the first content output unit 40.

[0053] The content storage unit 60 is mounted to the first content output unit 40 or the second content output unit 50 and stores data which is downloaded from the content supply unit 30.

[0054] In the meantime, the digital content recorded in the content storage unit 60 is reproduced through the first content output unit 40 or the second content output unit 50.

[0055] The record/reproduction apparatus supply unit 20 transmits the first registration request signal 22 to the authorization recognition unit 10, and receives the manufacturer key(MK_{PD}) and the manufacturer key data ($Cert_{AC}(MK_{PD})$) generated by the first registration request signal 22.

[0056] The content supply unit 30 transmits the second registration request signal 31 to the authorization recognition unit 10, transmits the first authentication qualification key data 11 qualified for providing an encoded digital content generated by the second registration request signal, and receives the second table generated from the authorization recognition unit 10.

[0057] The first content output unit 40 transmits the second registration request signal 41 to the content supply unit 30, and receives the second authentication qualification key($PubKey_{ISP}$) and the second authentication qualification key data($Cert_{CA}(PubKey_{ISP})$) and the private key($PrvKey_{LCM}$) and the public key($PubKey_{LCM}$) of the first content output unit 40 and the identifier(ID_{LCM}).

[0058] Further, the first content output unit 40 inputs the manufacturer key data($Cert_{CA}(MK_{PD})$) from the second content output unit 50 and transmits the same to the content supply unit 30. Furthermore, the first content output unit 40 extracts and encodes only table data corresponding to the manufacturer key data from the second table, and transmits the encoded table data to the second content output unit 50.

[0059] Therefore, the second content output unit 50 inputs and stores the manufacturer key(MK_{PD})and the manufacturer key data($Cert_{CA}$ (MK_{PD})) transmitted by the authorization recognition unit 10. Further, the second content output unit 50 transmits the manufacturer key data($Cert_{CA}(MK_{PD})$) to the content supply unit 30 through the first content output unit 40, and the second content output unit 50 inputs and interprets the manufacturer key data of the second table transmitted from the first content output unit 40 to store the internal memory.

[0060] Operations of the system for preventing an illegal copy of a digital content according to an embodiment of the present invention structured as above will be described in detail with reference to the accompanying drawings.

[0061] Figure 3 to Figure 5 are views for explaining key and key data flow for a case that respective blocks applied to Figure 1 request a registration or reproduce a digital content.

[0062] The accompanying drawings, Figure 3 to Figure 5 are views for showing a concrete embodiment of the present invention, terms employed in the present invention are briefly explained as follows.

[0063] Firstly, the authorization recognition unit 10, as a certificate authority(CA), enables the content supply unit 30 to provide a digital content, and enables the first content output unit 40 and the second content output unit 50 to receive the digital content, to thereby recognize an authorization.

[0064] Secondly, the record/reproduction apparatus supply unit 20, as a manufacture(MA), manufactures the second content output unit 50 to be provided to users.

[0065] Thirdly, the content supply unit 30, as an internet service provider(ISP), provides various data to users as well as a digital content, fourthly, the first content output unit 40, as a licensed SDMI compliant module, is a device which users can use like a general personal computer, the second content output unit 50 is a unit like an MP3 player, and the content storage unit 60 is a smart media card.

[0066] Explaining the embodiment of the present invention from now on, first of all, the record/reproduction apparatus supply unit 20 transmits the first registration request signal 22 to the authorization recognition unit 10 in order to download a digital content to a manufactured second content output unit 50 for reproduction.

[0067] Then, the authorization recognition unit 10 generates a manufacturer key(MK_{PD}) and a manufacturer key data ($Cert_{CA}$ (MK_{PD})), which the second content output unit 50 can uniquely have, to be transmitted to the record/reproduction apparatus supply unit 20.

[0068] Different manufacturer key(MK_{PD}) and different manufacturer key data($Cert_{CA}(MK_{PD})$) are generated from every second content output unit 50 which is registration-requested by the record/reproduction apparatus supply unit 20.

[0069] Therefore, the record/reproduction apparatus supply unit 20 stores the manufacturer key(MK_{PD}) and the manufacturer key data ($Cert_{CA}$ (MK_{PD})) recognized from the authorization recognition unit 10 in a temporary register area of the second content output unit 50 without other users' notice.

[0070] The authorization recognition unit 10 generates the manufacturer key(MK_{PD}) and the manufacturer key data($Cert_{CA}(MK_{PD})$) as well as randomly generates a token at the same time which are provided to the record/reproduction apparatus supply unit 20 as stated above.

[0071] That is, the authorization recognition unit 10 has two tables. The first table is a table which the authorization recognition unit 10 has and which has the manufacturer key(MK_{PD}) and the manufacturer key data ($Cert_{CA}(MK_{PD})$) as stated above.

[0072] Further, the second table is a manufacturer key data table which is transmitted to the content supply unit 30 by the authorization recognition unit 10 and which has the identifier(ID_{LCM}) of the second content output unit 50, the token encoded by the manufacturer key, and data for the token (refer to Figure 3).

[0073] Therefore, the second content output unit 50, which is manufactured and supplied from the record/reproduction apparatus supply unit 20, downloads and reproduces the digital content which is provided from the content supply unit 30.

[0074] Further, the content supply unit 30, like the record/ reproduction apparatus supply unit 20, can provide a digital content to the first content output unit 40, the second content output unit 50, and the content storage unit 60 due to an authorization recognition from the authorization recognition unit 10.

[0075] As stated above, the content supply unit 30 transmits the second registration request signal 31 to the authorization recognition unit 10 in order to recognize a digital content supply authorization.

[0076] Therefore, the authorization recognition unit 10, as shown in Figure 3, generates the first authentication qualification key ($PubKey_{ISP}$) and the first authentication qualification key data($Cert_{CA}(PubKey_{ISP})$).

[0077] That is, if the second registration request signal 31 is inputted from the content supply unit 30, the authorization recognition unit 10 temporarily forms a plurality of keys ($PrvKey_{eph}$, $PubKey_{eph}$) in order to form a secret channel between the content supply unit 30.

[0078] Further, the authorization recognition unit 10 generates the private key($PrvKey_{ISP}$), the public key ($PubKey_{ISP}$) as the second authentication qualification key, and the second public key data as the second authentication qualification key data($Cert_{CA}(PubKey_{ISP})$) in order for the content supply unit 30 to perform an authorization.

[0079] At this time, the second authentication qualification key and the second authentication qualification key data are encoded as the channel key(k) and provided to the content supply unit 30 through the secret channel formed between the authorization recognition unit 10 and the content supply unit 20. Here, the secret channel is formed by the channel key(k) which the authorization recognition unit 10 and the content supply unit 20 are shared.

[0080] In the meantime, since the secret channel is safely formed, illegal users can not download any data which is transmitted and received through the secret channel.

[0081] Therefore, since the content supply unit 30 interprets and stores in a storage unit data which is transmitted from the authorization recognition unit 10, the digital content can be downloaded to the first content output unit 40, the second content output unit 50, or the content storage unit 60.

[0082] Further, the first content output unit 40 transmits the third registration request signal to the content supply unit 30 passing through the processes as stated above. Furthermore, the content supply unit 30 transmits the public key($PubKey_{ISP}$) and the public key data ($Cert_{CA}(PubKey_{ISP})$) as the second authentication qual-

ification key and the second authentication qualification key data to the first content output unit 40, and the first content output unit 40 stores the public key($PubKey_{ISP}$) and the public key data($Cert_{CA}(PubKey_{ISP})$).

[0083] In the meantime, the channel key(k) is mutually shared between the content supply unit 30 and the first content output unit 40, and the first content output unit 40 safely receives the digital content through the secret channel generated by the shared channel key(k).

[0084] Further, the content supply unit 30 generates the private key($PrvKey_{LCM}$) and the public key($PubKey_{LCM}$) of the first content output unit 40 and identifier (ID_{LCM}), such generated data is encoded to the channel key(k) which is transmitted to the first content output unit 40. Furthermore, the first content output unit 40 interprets and stores the transmitted data by using the channel key(k).

[0085] At this time, if the second content output unit 50 is connected to the first content output unit 40, the first content output unit 40 generates and encodes by using the token a secret channel key(CK_{PD-LCM}) which is shared with the second content output unit 50 and which is transmitted to the second content output unit 50.

[0086] At this time, the token can be extracted from data which is read from the second table of the content supply unit 30 and encoded by the second authentication qualification key($PubKey_{LCM}$) and transmitted to the first content output unit 40.

[0087] That is, a brief description for extracting the roken(T) will be as follows. Since the encoded data which is transmitted to the first content output unit 40 is interpreted by the second authentication qualification key ($PubKey_{LCM}$) which is stored in the first content output unit 40, the first content output unit 40 can obtain the token(T) and the token data(T*).

[0088] The token data(T*) is a token(T) which is encoded by the manufacturer key(MK_{PD}).

[0089] Such interpreted token(T) from the first content output unit 40 is used in encoding the secret channel key(CK_{PD-LCM}), and the token data(T*) is transmitted to the second content output unit(50).

[0090] At this time, the token data(T*) which is transmitted to the second content output unit 50 is interpreted by the manufacturer key(MK_{PD}) which is stored in the second content output unit 50, and the second content output unit 50 extracts the token (T). Further, the second content output unit 50 interprets the encoded channel key(k) which is transmitted from the first content output unit 40 by using the extracted token and stored in the internal memory.

[0091] Therefore, the second content output unit 50 stores the transmitted channel key(k) as well as encodes the registered manufacturer key data to the second authentication qualification key($PubKey_{LCM}$) of the first content output unit 40 which is transmitted to the content supply unit 30.

[0092] In the meantime, the content supply unit 30 interprets data which is transmitted through the first content output unit 40 and compares the interpreted manufacturer key data and data of the second table. If there is the corresponding data, the content supply unit 30 encodes the token(T) and the token data(T*) of the table contents into the second authentication qualification key ($PubKey_{LCM}$) and then transmits the second authentication qualification key($PubKey_{LCM}$) to the first content output unit 40.

[0093] Therefore, the content supply unit 30 can download the digital content to the first content output unit 40 and the second content output unit 50, and the first content output unit 40 and the second content output unit 50 can reproduce the downloaded digital content.

[0094] As stated above, in order to prevent an illegal copy as the digital content which is downloaded from the content supply unit 30 according to the request of the first content output unit 40 is again downloaded to the second content output unit 50, the internet appliance 40 has a database(RMS-DB; Right Management System-Data Base) which can check a present state of the digital content together with the digital content (refer to Figure 5).

[0095] The database contains an identifier data area of the digital content, an updated token data area, a data area for checking a present state of the digital content, and a reproduction control data area.

[0096] Further, the database is stored in the first content output unit 40 in an encoded form by the secret channel key(CK_{PD-LCM}) which the first content output unit 40.

[0097] The most important area in the database (RMS-DB) is the updated token area(UTD), and the updated token area(UTD) has different values when the updated token area(UTD) downloads a digital content from the first content output unit 40 to the second content output unit 50, or uploads the digital content from the second content output unit 50 to the first content output unit 40.

[0098] At this time, the updated token is transmitted to the first content output unit 40 through the second content output unit 50 to update the stored token in the first content output unit 40.

[0099] That is, data registered in the database(RMS-DB) of the first content output unit 40 becomes different every time the first content output unit 40 reproduces, downloads, or updates a digital content downloaded into the first content output unit 40. Therefore, the first content output unit 40 checks the registered data in the database if users legally use the digital content in the case that a request signal for reproduction, dowload, or upload of the digital content is inputted by the users.

[0100] Further, in the case that the digital content is downloaded or uploaded between the first content output unit 40 and the second output unit 50, an area is checked which has data for checking a present state of the digital content and which is the second area of the

database(RMS-DB).

[0101] That is, since the first content output unit 40 checks the third area, when the second content output unit 50 downloads a digital content downloaded from the first content output unit 40 to the second content output unit, the selection of a copy form or a transmission form can be read.

[0102] Further, by checking check-in/check-out data included in the second area, the transmission state of the digital content can be read. That is, the check-in data means that a digital content is not downloaded from the first content output unit 40 to the second content output unit 50.

[0103] The check-out data means that the digital content is a downloading state from the first content output unit 20 to the second content output unit 50, or that the downloaded digital content is again uploaded to the first content output unit 40.

[0104] The last area of the database (RMS-DB) is a reproduction control data area and contains data for reproduction times of a digital content, a reproduction expiration period of the digital content, and an amnesty period of the digital content.

[0105] Here, the reproduction times of the digital content is a value which is established when a digital content is provided from the content supply unit 30 to the first content output unit 40 and which controls the reproduction times by counting down one by one every time the digital content is downloaded.

[0106] Further, the reproduction expiration period of the digital content does not mean the reproduction of the digital content and the control of the output state, but a period established by the content supply unit 30, and the digital content downloaded from the content supply unit 30 to the first content output unit 40 can be reproduced in the period as stated above.

[0107] Lastly, the amnesty period of the digital content enables the digital content downloaded from the content supply unit 30 to the first content output unit 40 to be reproduced irrespectively of the reproduction times of the digital contents or the expiration period.

[0108] As stated above, if the content supply unit 30 accepts a download request of a digital content of the first content output unit 40, the content supply unit 30 firstly identifies the ID of the first content output unit 40, judges as the first content output unit 40 legally connected to the content supply unit 30, and downloads a digital content having a file format embodied by the secret system to the first content output unit 40.

[0109] The file format having a digital content transmitted to the first content output unit 40 from the content supply unit 30, as shown in Figure 6, contains a title ID field, a content discription field(CDF), algorithm identifying field(AIF), an indicator of source originator field (SOI), a copyright holder information field(CHI) indicating a copy holder information, a right management field (RMF), a content encription key(CEK), and a digital content field encoded to a content encryption key.

[0110] The content discription field has data such as a digital content composer, a singer, a record label or the like.

[0111] The algorithm identifying field denotes an algorithm employed in the secret system embodied in the present invention, and there are ECC, SNAKE, CODEC and the like in the algorithm.

[0112] The SOI field has one of data of ISP_ID denoting an identifier of a content supply unit 30 of the present invention, LSP_ID denoting an identifier of the first content output unit 40, PD_ID denoting an identifier of the second content output unit 50.

[0113] Therefore, in the case that the first content output unit 40 downloads and reproduces a digital content having the format as stated above, firstly an algorithm encoded from the AIF field is identified, and the authentication qualification of the first content output unit 40 is recovered by using the identified encryption algorithm.

[0114] Further, the identifier which the first content output unit 40 has and the identifier in the SOI field of the file format are compared to check if there is correspondence between the two. In the case of correspondence, the copy control state from the RMF data, the reproduction control state, and the transmission control state are identified to register them in the database (RMS-DB) which the first content output unit 40 has.

[0115] After the above process is performed, a digital content encryption key is extracted by using a CEK field, and the encoded digital content is interpreted by using the encryption key.

[0116] At this time, in the case that the first content output unit 40 does not violate any one of the above, the content supply unit 30 judges that the first content output unit 40 is legal, and downloads the digital content.

[0117] In the case of changing the RMF field of the file formats, in particular the reproduction control state, the first content output unit 40 replaces the reproduction control state data in two places of the database(RMS-DB) and the file format with desired data.

[0118] Further, as stated above, in the case that a digital content downloaded from the first content output unit 40 is again downloaded to the second content output unit 50, the following processes are required.

[0119] Firstly, the first content output unit 40 receives the UTD data which the second content output unit 50 of the identifier of the second content output unit by a request to the second content output unit 50.

[0120] Therefore, the second content output unit 50 encodes the UTD into the third channel key($CK_{PD\text{-}LCM}$) shared with the first content output unit 40 and the third channel key($CK_{PD\text{-}LCM}$) is transmitted to the first content output unit 40 together with the identifier of the second content output unit.

[0121] At this time, the first content output unit 40 identifies data transmitted from the second content output unit 50 and extracts the identifier of the second content output unit 50 and the UTD from the transmitted data by using the channel key($CK_{PD\text{-}LCM}$) shared with the

second content output unit 50, and compares the extracted identifier of the second content output unit 50 and the UTD with data registered in the database.

[0122] If the UTD is unchanged and the RMF is changed, the first content output unit 40 updates the two places of the database and the file format to the changed RMF.

[0123] That is, the first content output unit 40 updates the database to a newly generated UTD, and the updated UTD is encoded by the channel key(CK_{PD-LCM}) and the encoded channel key(CK_{PD-LCM}) is transmitted to the second content output unit 50.

[0124] In the meantime, the first content output unit 40 transmits a digital content to the second content output unit 50, and data of an initial transmission control state field is 'Transfer'. As the digital content is transmitted to the second content output unit 50, data of the transmission control state field is changed to 'Transferred'.

[0125] As stated above, changed data of the transmission control state field is updated in the database (RMS-DB), and is not changed in the file format. At this time, the transmission control state field has three types of 'Transfer', 'Transferred', and 'Transfer-non'.

[0126] Next, as a digital content is transmitted to the second content output unit 50 from the first content output unit 40, data for the copy control state field is initially set to the check-in in the database as well as in the file format, but after the digital content is transmitted, the data for the copy control state field is changed to the check-out both in the database and the file format.

[0127] If the data for the copy control state field is set to 'Copy-never', users using the system of the present invention can not download the digital content of the first content output unit 40 to the second content output unit 50.

[0128] If the above processes are correctly performed, the digital content is downloaded to the second content output unit 50.

[0129] Figure 7 is a view for preventing an illegal copy in downloading to the content storage unit 60 a digital content which the second content output unit 50 has. Firstly, the second content output unit 50 transmits to the content storage unit 60 an encoded digital content to be recorded in the content storage unit 60 and an encoded reproduction data to reproduce the digital content.

[0130] At this time, another encryption of data necessary to produce the encoded digital content is performed as follows.

[0131] That is, the second content output unit 50 contains a random number generation unit(RNG) for randomly generating a number, and a function process unit (F) for function-processing various inputs and generating predetermined values which only the content storage unit 60 can have.

[0132] At this time, values inputted to the function process unit(F) are a random number, a channel key, and a bad sector address and an inherent number which the content storage unit 60 inherently has.

[0133] Further, another encryption of an encoded digital content reproduction data is performed by using function values generated in the function process unit (F).

[0134] A digital content referred to in the present invention is downloaded from the first content output unit 40 to the second content output unit 50 and the content storage unit 60, or uploaded from the second content output unit 50 to the first content output unit 40. This is denoted by checking a field indicating transmission control state data of file format data which is provided from the database and the content supply unit 30 which the first content output unit 40.

[0135] If, as stated above, 'transfer' is indicated as a result that the first content output unit 40 checks the database and the transmission control state data field of the file format, the first content output unit 40 can download a digital content to the second content output unit 50, if the digital content is downloaded from the first content output unit 40 to the second content output unit 50, 'transfer' is changed to 'transferred' in the database and the transmission control state data field of the file format and the changed data is transmitted to the second content output unit 50.

[0136] Further, since the digital content downloaded to the second content output unit 50 is not in the first content output unit 40, in order to be again reproduced in the first content output unit 40, the digital content is again uploaded from the second content output unit 50 to the first content output unit 40.

[0137] However, the digital content downloaded to the content storage unit 60 from the first content output unit 40 can be reproduced in an arbitrary second content output unit 50. Further, the digital content downloaded to the content storage unit 60 is uploaded to another first content output unit 40 through the second content output unit 50.

[0138] Furhter, various input devices are additionally connected to the first content output unit 40 and the second content output unit 50 applied to the present invention, and such input devices are shown in detail in Figure 8.

[0139] That is, the input devices which can be additionally connected to the first content output unit 40 and the second content output unit 50 can be CD such as RedBook CD, audio CD, super audio CD, DVD Disk, and analog input, and the like.

[0140] The audio signal inputted through the input devices is inputted to the first content output unit 40, and encoded according to a system supported in the present invention, and then transmitted to the second content output unit 50, or transmitted to the content storage unit 60 to be reproduced through the second output unit 50.

[0141] In the meantime, Kiosk in Figure 8 is a unit of an intermediate property of the content supply unit 30 and the first content output unit 40. The kiosk generates

a registration request signal for selling an encoded digital content by the content supply unit 30 through a PC connected with an internet.

[0142] Therefore, the content supply unit 30 provides to the kiosk the storage medium having a digital content encoded by a system supported in the present invention according to the registration request signal, and the kiosk receives fees from users and transmits a digital content stored in the storage medium.

[0143] Figure 9 is a view for explaining an input control of the output source of Figure 8.

[0144] As shown in Figure 9, applied program interface(API) of the first content output unit(indicated as 'Host' in Figure 9) checks if data inputted through the CD, EMD(content provided over internet), PM, DVD, and the like(hereinafter, referred to as 'input devices') can be reproduced in a system supported in the present invention.

[0145] Therefore, if the data can be reproduced in the system supported in the present invention, the API converts data inputted from the input devices to a format which can be reproduced in the system.

[0146] In the meantime, as a method which data can be reproduced in the system supported in the present invention as stated above, first, in the case that the input devices are the super CD or DVD, data which checks if data recorded on the storage medium can be copied is in an area out of data area. The API detects the area and uses the data when converting a signal inputted to the first content output unit('40' in Figure 1) to a file format supported in the present invention.

[0147] Secondly, in the case that the input device is the EMD and data inputted through the EMD has an encoded format, the API detects an encryption key and an encryption algorithm and uses the data when converting a signal inputted to the first content output unit 40 to a file format supported in the present invention.

[0148] Thirdly, if the input device is a general analog input, the API encodes inputted data according to a system supported in the present invention.

[0149] In the meantime, the API checks if an input device and data inputted from the input devices are suitable for the system and transmits the following data to the import control layer.

[0150] First, data for the type of a storage medium, for example, data for a type of an input device such as audio CD, DVD and the like, second, data for an initial form of data inputted to the first content output unit 40 from an input device, for example, data for a title, a player, a singer and the like, third, data for an encryption key which is data for an encryption algorithm.

[0151] At this time, the data is transmitted to the second content output unit 50 from the first content output unit 40 through the first interface part. Further, the data inputted from the third interface part of the second content output unit 50 is inputted to the import control layer of the second content output unit to be restructured in a file format shown in Figure 6.

[0152] That is, the file format in Figure 6 formed in the import control layer of the second content output layer 50 indicates data for a storage medium in the title-ID field, data for initial data inputted to an internet appliance from an input device for the CDF, data for an encryption algorithm outputted to the import control layer from the API of the first content output unit for the AIF, LCM-ID in the Device-ID field and SOI field, data for a copyright protection in the CHI field, and following data for the RMF.

[0153] First of all, 'copy not available' is indicated for the copy control state, 'check-in/check-out' is selectively indicated for the download/upload, 'reproduction times=no limit or predetermined times' is selectively indicated for the reproduction control state, and 'transmission not available' is indicated for the reproduction control state since the copy control state is 'copy not available'.

[0154] Next, CEK=k field which is a field indicating data for an encryption key, if an inputted digital content is not encoded, randomly generates a key(k), and a digital content inputted from the first content output unit is encoded by the key(k) and indicated in the last field(ENC (k, Content)).

[0155] At this time, the first content output unit 40, if data inputted through an input device is encoded, judges what algorithm is used for encryption, and checks an encryption algorithm which the second content output unit 50 to transmit an encoded digital content has.

[0156] Accordingly, if two algorithms are not matched, the first content output unit 40 interprets an encoded digital content and performs a trans-cypted process which again encodes the digital content with encryption/decryption algorithm which the second content output unit 50 has.

[0157] In the meantime, in the file format formed through the process, there is a secret header portion shown in Figure 6 from the Device-ID field to the field which indicates the encryption key. The secret header is encoded by the second authentication qualification key($PubKey_{LCM}$) which the first content output unit 40 has.

[0158] In the meantime, the first interface part in the first content output unit 40 checks if the second content output unit('50' in Figure 1) has an identifier and the third channel key($CK_{PD\text{-}LCM}$) and identifies if the qualification is an authenticated second content output unit 50.

[0159] In the meantime, an analog input inputted to the second content output unit 50 is inputted to the import control layer of a PDFM(PD Functional Module) in the second content output unit 50, and the analog input is converted to a file format supported in the present invention by a process described later.

[0160] Here, the import control layer, if the analog input is received by frame unit, first encodes the frame, encodes the encoded frame by using a randomly generated key, and if all frames are encoded, a file format as shown in Figure 6 is formed for preventing a copy for

an encoded analog input.

[0161] In order to prevent an illegal copy as shown in Figure 6, as in data indicated for RMF, an encoded analog input has a detailed information.

[0162] That is, 'copy not available' is indicated for the copy control state, 'check-in/check-out' is selectively indicated for the download/upload, 'reproduction times=no limit or predetermined times' is selectively indicated for the reproduction control state, and 'transmission not available' is indicated for the reproduction control state.

[0163] Further, data of the Device-ID field and the SOI field which are prepared before the RMF is indicated as 'PD_ID'.

[0164] The secret header portion generated via the above process is encoded by the third channel key ($CK_{PD\text{-}LCM}$) which the second content output unit 50 has.

[0165] At this time, the second content output unit 50 transmits the encoded digital content to the content storage unit 60, since a digital content which is transmitted to the content storage unit 60 does not indicate the SOI field data as an identifier which the content storage unit 60 has but as 'PD-ID' as stated above, the digital content can not be reproduced via arbitrary second output unit 50.

[0166] That is, a digital content recorded on the content storage unit can be reproduced only in the second content output unit 50 which has the same identifier as 'PD-ID' data of the SOI field contained in the content.

[0167] Accordingly, as stated above, in the present invention, entire system shares a channel key between units performing mutual communication, forms a safe channel, mutually transmits and receives a digital content, and prevents illegal users from taking the digital content on the way. Further, even though legal users legally downloads a digital content, since the second content output unit has the above structure, illegal copy of a digital content between the second content output unit as well as the content storage unit is prevented.

[0168] As stated above, preferred embodiments of the present invention are shown and described. Although the preferred embodiments of the present invention have been described, it is understood that the present invention should not be limited to these preferred embodiments but various changes and modifications can be made by one skilled in the art within the spirit and scope of the present invention as hereinafter claimed.

[0169] The reader's attention is directed to all papers and documents which are filed concurrently with or previous to this specification in connection with this application and which are open to public inspection with this specification, and the contents of all such papers and documents are incorporated herein by reference.

[0170] All of the features disclosed in this specification (including any accompanying claims, abstract and drawings), and/or all of the steps of any method or process so disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive.

[0171] Each feature disclosed in this specification (including any accompanying claims, abstract and drawings), may be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

[0172] The invention is not restricted to the details of the foregoing embodiment(s). The invention extend to any novel one, or any novel combination, of the features disclosed in this specification (including any accompanying claims, abstract and drawings), or to any novel one, or any novel combination, of the steps of any method or process so disclosed.

Claims

1. A system for preventing an illegal copy of digital contents, comprising:

   authorization recognition means (10) for generating a first authentication qualification key and a first authentication qualification key data in response to an externally input second registration request signal;

   content supply means (30) for transmitting the second registration request signal to the authorization recognition means (10), storing a first authentication qualification key and the first authentication qualification key data input from the authorization recognition means (10), and generating a second authentication qualification key and a second authentication qualification key data; and

   first content output means (40) for outputting a third registration request signal to the content supply means (30), and storing the second authentication qualification key and the second authentication qualification key data input from the content supply means (30).

2. The system as claimed in claim 1, wherein the authorization recognition means (10) forms a first channel key capable of sharing with the content supply means (30) in response tc a first registration request signal inputted from the content supply means (30), and outputs an encoded first authentication qualification key and an encoded first authentication qualification key data to the content supply means (30) via a secret channel formed by the first channel key.

3. The system as claimed in claim 2 or 3, wherein the content supply means (30) interprets and stores the first authentication qualification key and the first authentication qualification key data input from the authorization recognition means (10) via the secret channel by using the first channel key.

4. The system as claimed in claim 1, wherein the content supply means (30) forms a second channel key capable of sharing with the first content output means (40) in response to the second registration request signal input from the first content output means (40), and outputs a second authentication qualification key and an encoded authentication qualification key data to the first content output means (30) through a secret channel formed by the second channel key.

5. The system as claimed in claim 1 or 4, wherein the first content output means (40) interprets and stores the second authentication qualification key and the second authentication qualification key data inputted from the content supply means (30) through the secret channel by using the second channel key.

6. A system for preventing an illegal copy of digital contents, comprising:

authorization recognition means (10) for generating a manufacturer key and a manufacturer key data in response to an externally input first registration request signal, generating a first table and a second table by using the manufacturer key and the manufacturer key data, and generating a first authentication qualification key and a first authentication qualification key data in response to the second registration request signal inputted from external;

record/reproduction apparatus supply means (30) for outputting the first registration request signal to the authorization recognition means (10), and storing the manufacturer key and the manufacturer key data inputted from the authorization recognition means (10);

content supply means (30) for outputting the second registration request signal to the authorization recognition means (10), storing the first authentication qualification key, the first authentication qualification key data, and the second table, and generating a second authentication qualification key and a second authentication qualification key data in response to an externally input third registration request signal;

first content output means (40) for outputting the third registration request signal to the content supply means (30), storing the second authentication qualification key and the second authentication qualification key data input from the content supply means (30), outputting the externally input manufacturer key data to the content supply means (30), encoding and outputting the manufacturer key detected from the second table in response to the manufacturer key data; and

second content output means (50) for storing the manufacturer key and the manufacturer key data input from the authorization recognition means (10), outputting the manufacturer key data to the content supply means through the first content output means (40), and comparing the manufacturer key with the manufacturer key of the second table input from the first content output means (40) in order to judge if the stored manufacturer key is authenticated.

7. The system as claimed in claim 6, wherein the first table generated from the authorization recognition means (10) contains the manufacturer key data, the manufacturer key, and an identifier corresponding to the manufacturer key, and is stored only in the authorization recognition means (10).

8. The system claimed in claim 6 or 7, wherein the second table generated from the authorization recognition means (10) and output to the content supply means (30) has an identifier corresponding to the manufacturer key data and the manufacturer key, data from encryption of the manufacturer key by using a token, and a token.

9. The system claimed in claim 6, 7 or 8, wherein a content storage means (60) is further included which is connected to the first content output means (40) or the second content output means (50) and stores data downloaded from the content supply means (30).

10. The system claimed in claim 6, 7, 8, or 9, wherein the authorization recognition means (10) forms a first channel key capable of sharing with the content supply means (30) in response to a first registration request signal inputted from the content supply means, and outputs an encoded first authentication qualification key and an encoded first authentication qualification key data to the content supply means via a secret channel formed the first channel key.

11. The system claimed in any of claims 6 to 10, wherein the content supply means (30) forms a second channel key capable of sharing with the first content output means (40) in response to the second regis-

tration request signal input from the first content output means (40), and outputs a second authentication qualification key and an encoded authentication qualification key data to the first content output means (40) through a secret channel formed by the second channel key.

12. The system claimed in any of claims 6 to 11, wherein the first content output means (40) interprets and stores the second authentication qualification key and the second authentication qualification key data inputted from the content supply means (30) through the secret channel by using the second channel key.

13. The system claimed in claim 7, wherein the token is randomly generated by the authorization recognition means (10).

14. The system claimed in claim 6, wherein the first content output means (40) forms a third channel capable of being shared with the second content output means (50), encodes the third channel key with a token inputted from the content supply means (30) and transmits to the second content output means (50).

15. The system claimed in claim 6, wherein the second content output means (50) extracts a token from encoded manufacturer data from the first content output means (40) by using the stored manufacturer key in advance, interprets and stores the third channel key by using the token to form a secret channel with the first content output means (40).

16. A system for preventing an illegal copy of digital contents, comprising:

content supply means (30) for supplying an encoded digital content;

first content output means (40) including a database which has reproduction data of a digital content downloaded from the content supply means (30), encoding the database by using the third channel key for storage, interpreting the reproduction data of the digital content inputted from external by using the third channel key to be compared with a reproduction data of the database, to thereby judge if an illegal copy of the digital content is performed; and

second content output means (50) for updating the reproduction data of the digital content stored in advance by interpreting the reproduction data of the digital content input from the first content output means (40) by using the third channel key, and transmitting the updated reproduction data of the digital content to the first content output means.

17. The system claimed in claim 16, wherein the database is separated with an identifier data area of the digital content, an updated token data area, an data area for a present state of the digital content, and a reproduction control data area, and has the corresponding data.

18. The system claimed in claim 17, wherein the data area for the present state of the digital content includes:

data indicating that the digital content is downloaded in a copy form from the first content output means (40) to the second content output means (50);

data indicating that the digital content is downloaded in a transmission form from the first content output means (40) to the second content output means (50); and

data indicating that the digital content is downloaded and uploaded between the first content output means (40) and the second content output means (50).

19. The system claimed in claim 17, wherein the reproduction control data area of the digital content includes:

data for reproduction times of the digital content;

data for a reproduction expiration period of the digital content; and

data for an amnesty period of the digital content.

FIG.1

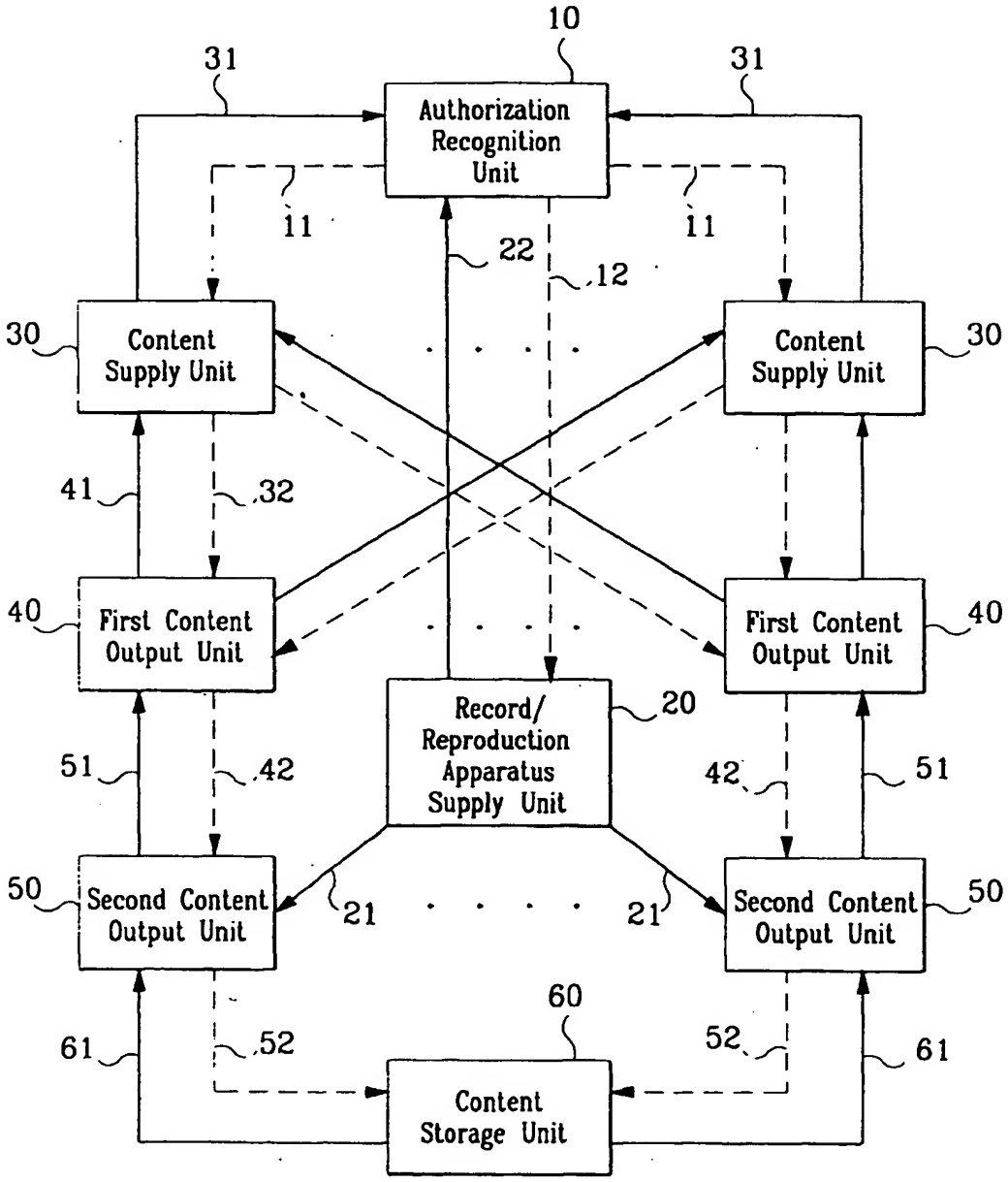

10
31
31
Authorization Recognition Unit
11
11
22
12
30
Content Supply Unit
Content Supply Unit
30
41
32
40
First Content Output Unit
First Content Output Unit
40
Record/ Reproduction Apparatus Supply Unit
20
51
42
42
51
50
Second Content Output Unit
21
21
Second Content Output Unit
50
60
61
52
52
61
Content Storage Unit

FIG.2

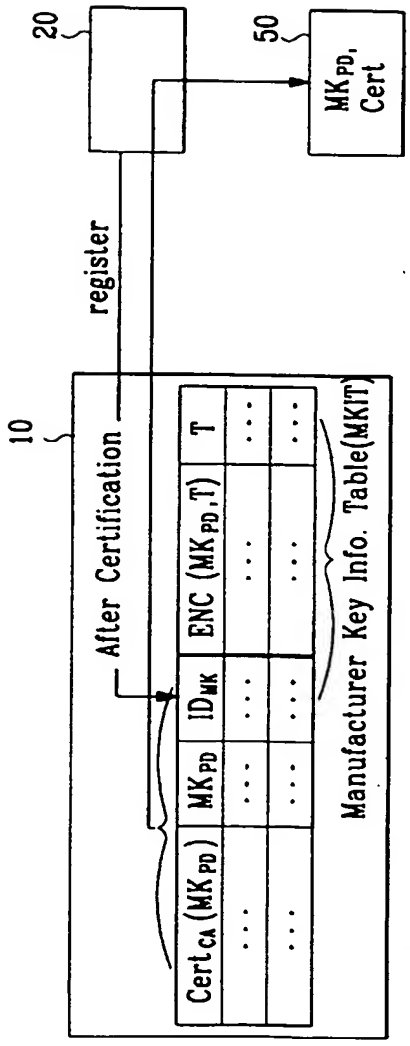

20
50
MK_{PD}, Cert
register
10
After Certification
$Cert_{CA}(MK_{PD})$
MK_{PD}
ID_{MK}
ENC (MK_{PD},T)
T
Manufacturer Key Info. Table(MKIT)

FIG.3

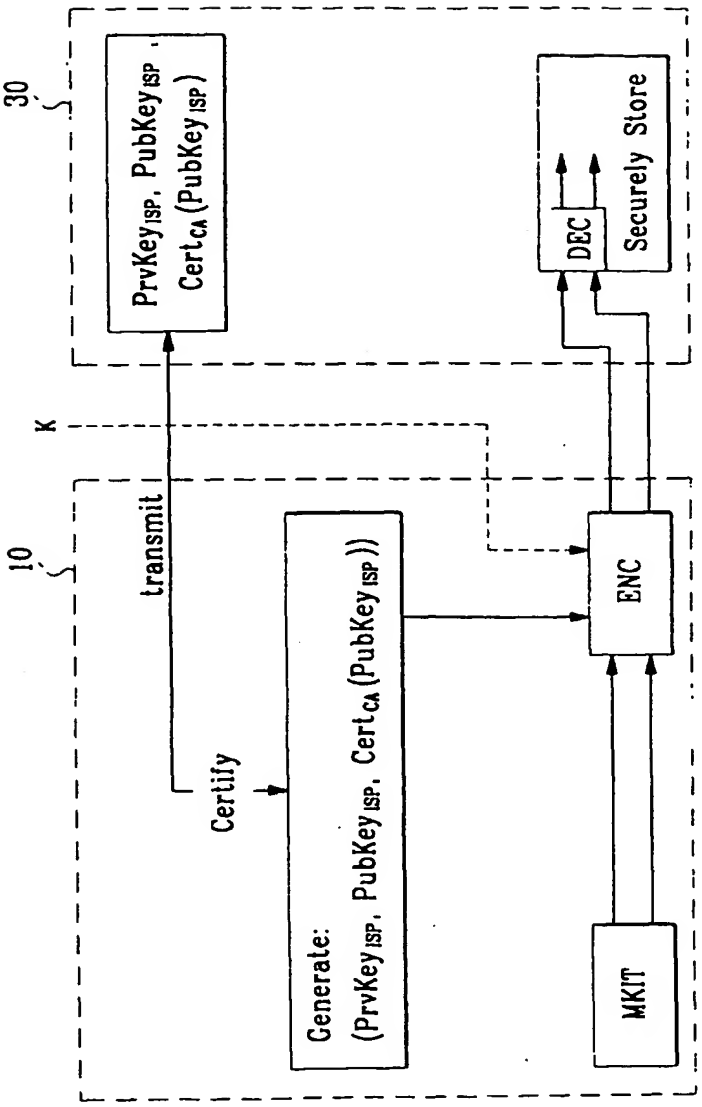

30
PrvKey ISP, PubKey ISP,
Cert CA (PubKey ISP)
DEC
Securely Store
K
10
transmit
Certify
Generate:
(PrvKey ISP, PubKey ISP, Cert CA (PubKey ISP))
ENC
MKIT

FIG.4

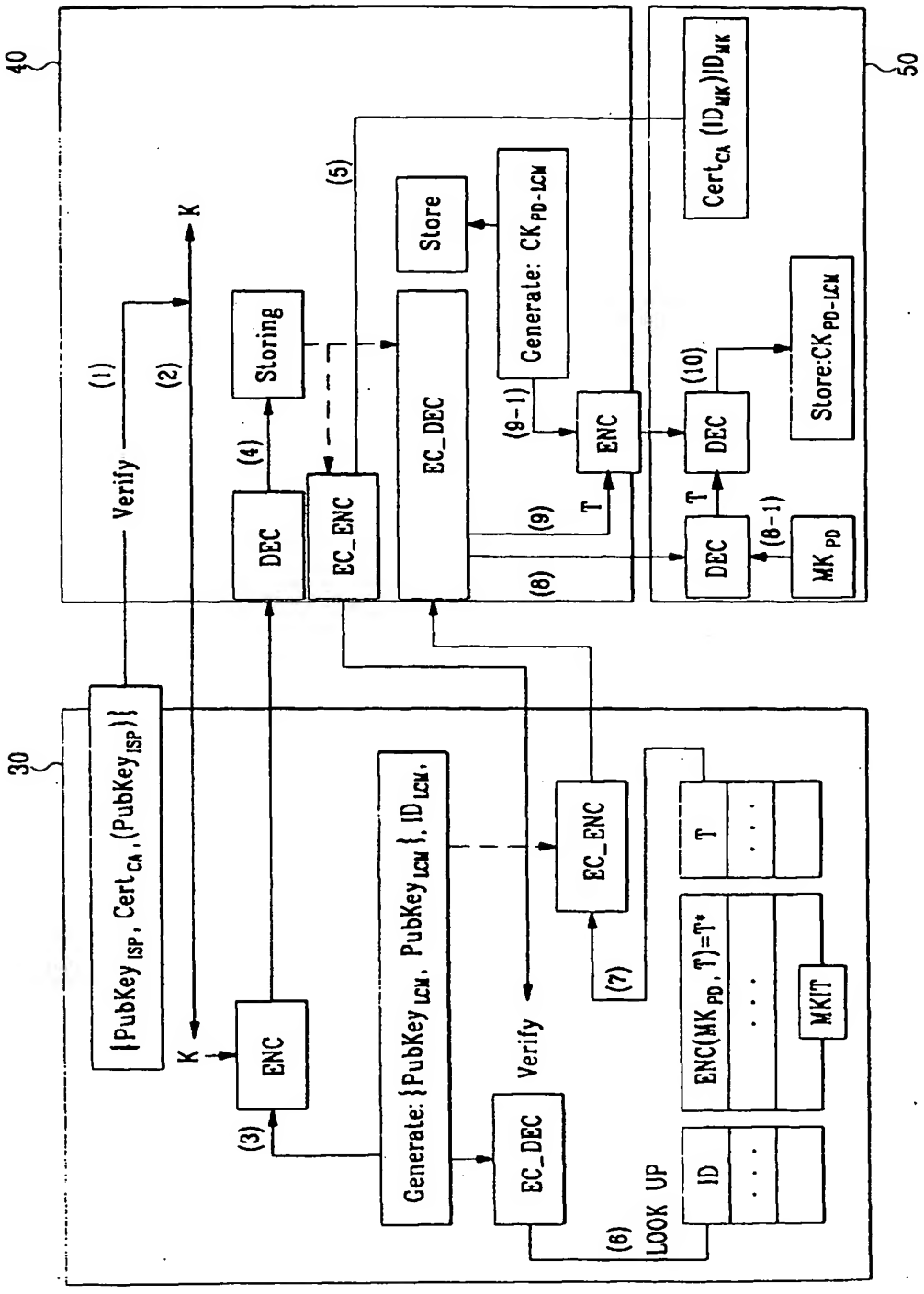

40
50
30
Verify
(1)
(2)
K
Storing
(4)
DEC
EC_ENC
(5)
EC_DEC
Store
Generate: CK PD-LCN
(9-1)
ENC
(9)
T
(8)
Cert CA (ID MK)ID MK
(10)
DEC
Store:CK PD-LCN
DEC
(8-1)
MK PD
{PubKey ISP, Cert CA, (PubKey ISP)}
K
ENC
(3)
Generate: {PubKey LCN, PubKey LCN}, ID LCN
EC_DEC
Verify
EC_ENC
(7)
T
ENC(MK PD, T)=T*
MKIT
ID
LOOK UP
(6)

FIG.5

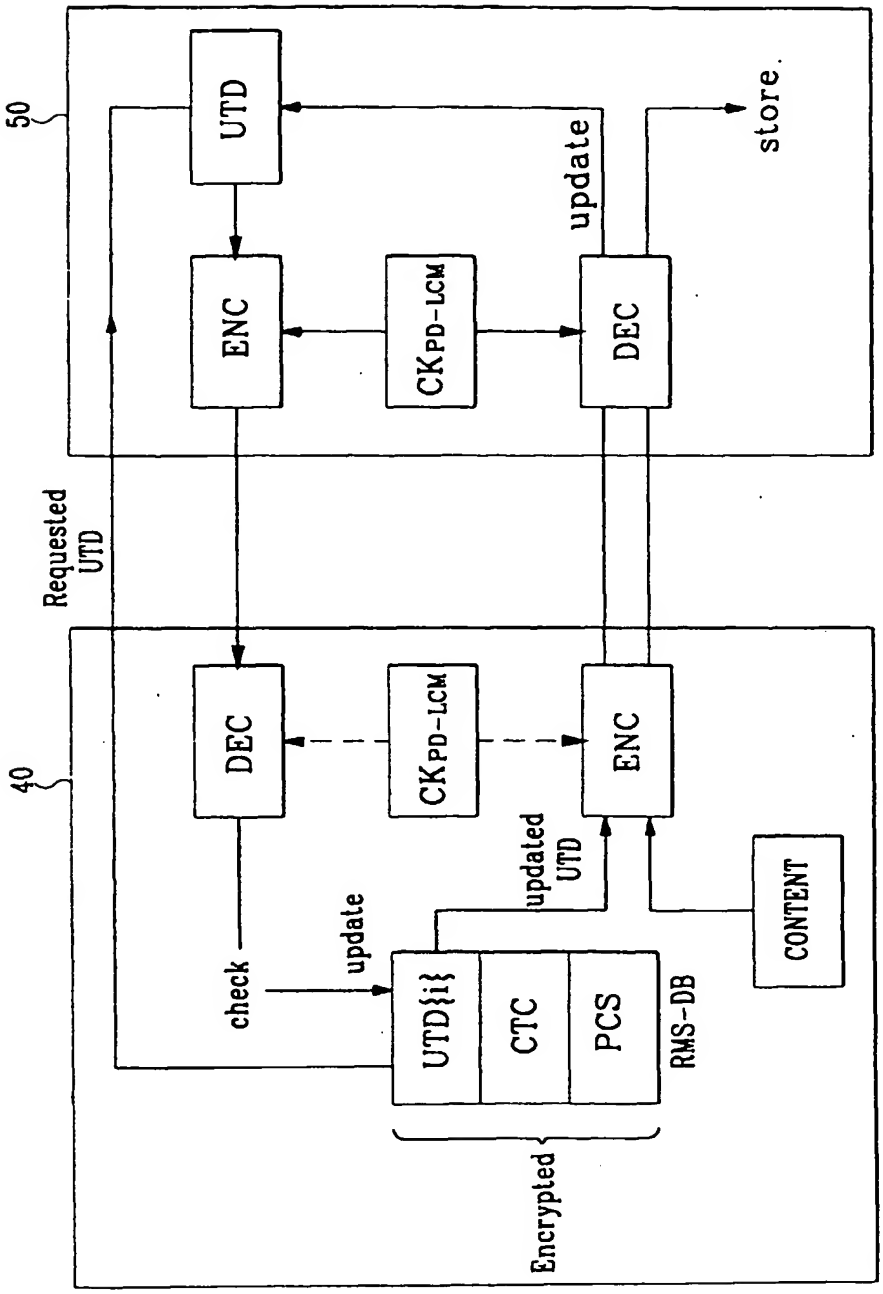

50
UTD
store
update
ENC
CKPD-LCM
DEC
Requested UTD
40
DEC
CKPD-LCM
ENC
updated UTD
CONTENT
update
check
UTD{i}
CTC
PCS
RMS-DB
Encrypted

FIG.6

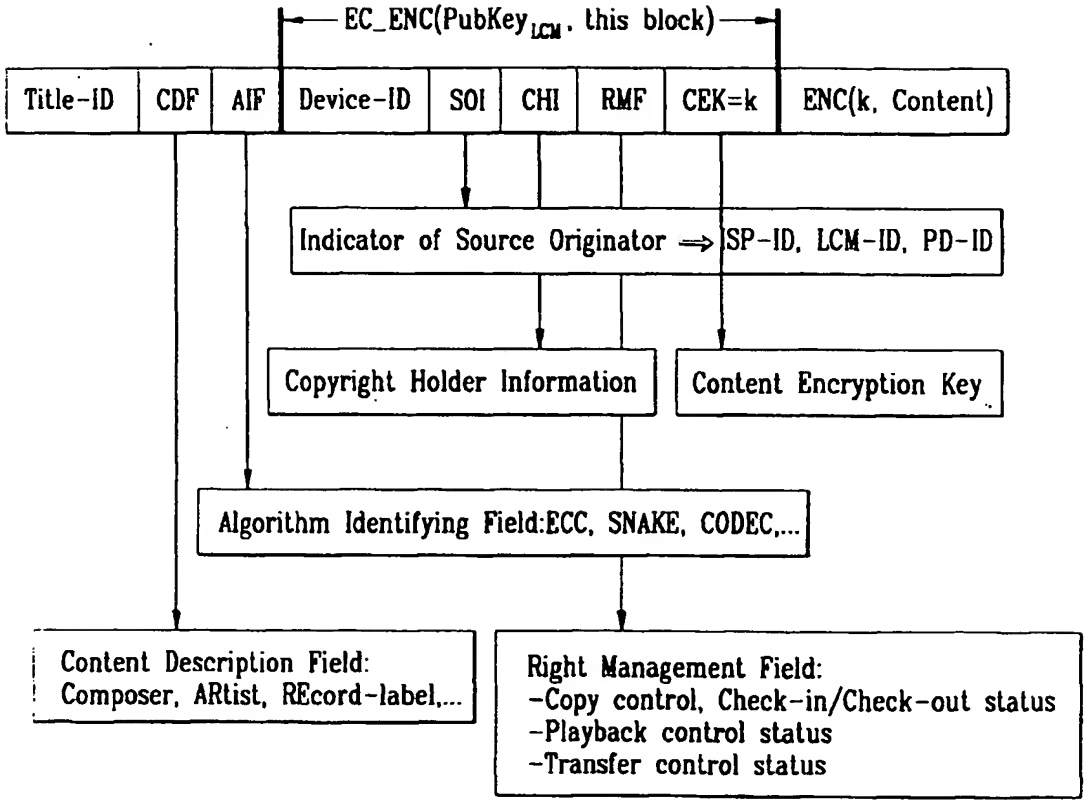

EC_ENC(PubKey LCM, this block)
Title-ID
CDF
AIF
Device-ID
SOI
CHI
RMF
CEK=k
ENC(k, Content)
Indicator of Source Originator ⇒ SP-ID, LCM-ID, PD-ID
Copyright Holder Information
Content Encryption Key
Algorithm Identifying Field:ECC, SNAKE, CODEC,...
Content Description Field:
Composer, ARtist, REcord-label,...
Right Management Field:
-Copy control, Check-in/Check-out status
-Playback control status
-Transfer control status

FIG.7

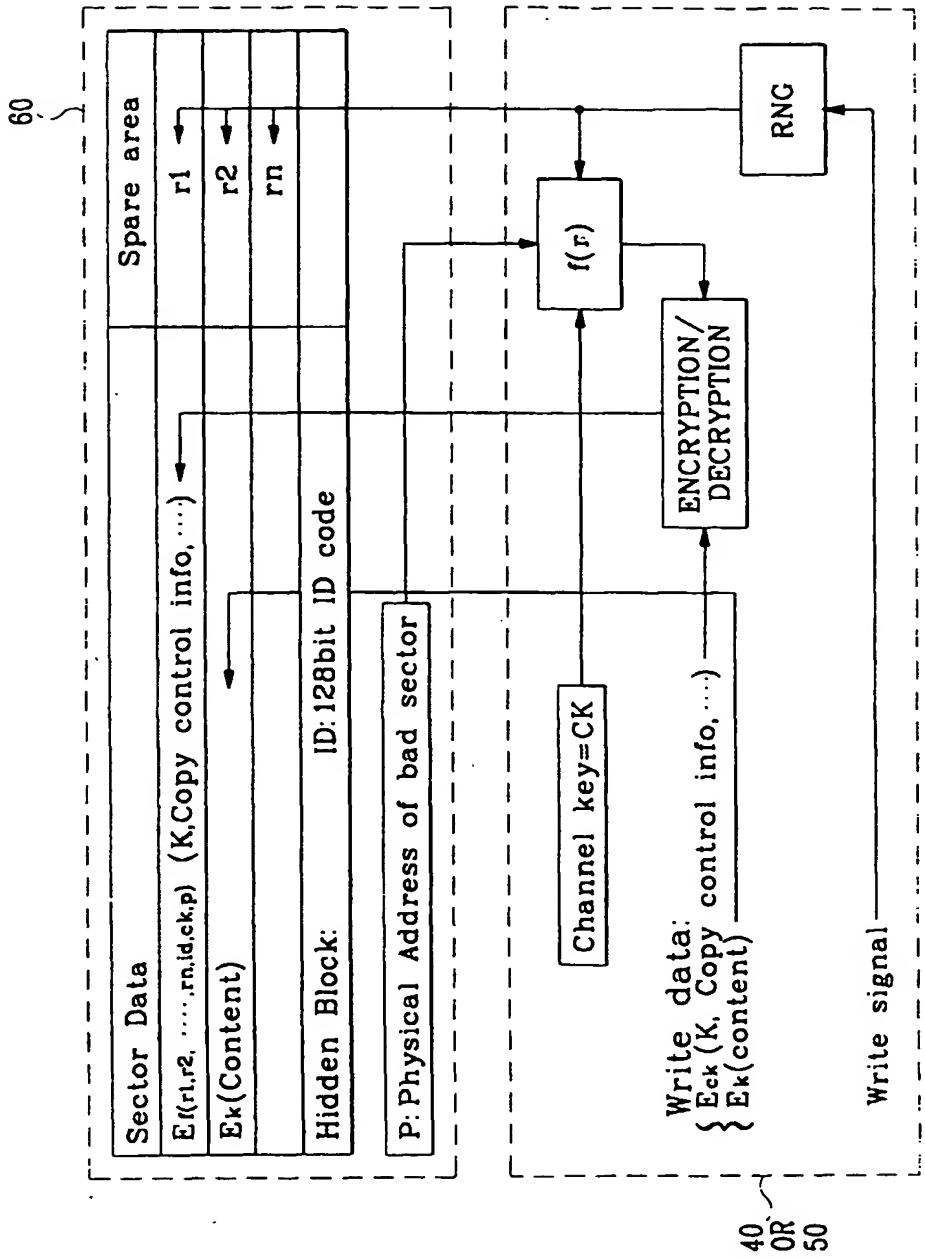

60
Spare area
r1
r2
rn
Sector Data
Ef(r1,r2, ····,rn,id,ck,p) (K,Copy control info,····)
Ek(Content)
Hidden Block:
ID:128bit ID code
P: Physical Address of bad sector
f(r)
RNG
ENCRYPTION/
DECRYPTION
Channel key=CK
Write data:
{ Eck(K, Copy control info,····)
{ Ek(content)
Write signal
40
OR
50

FIG.8

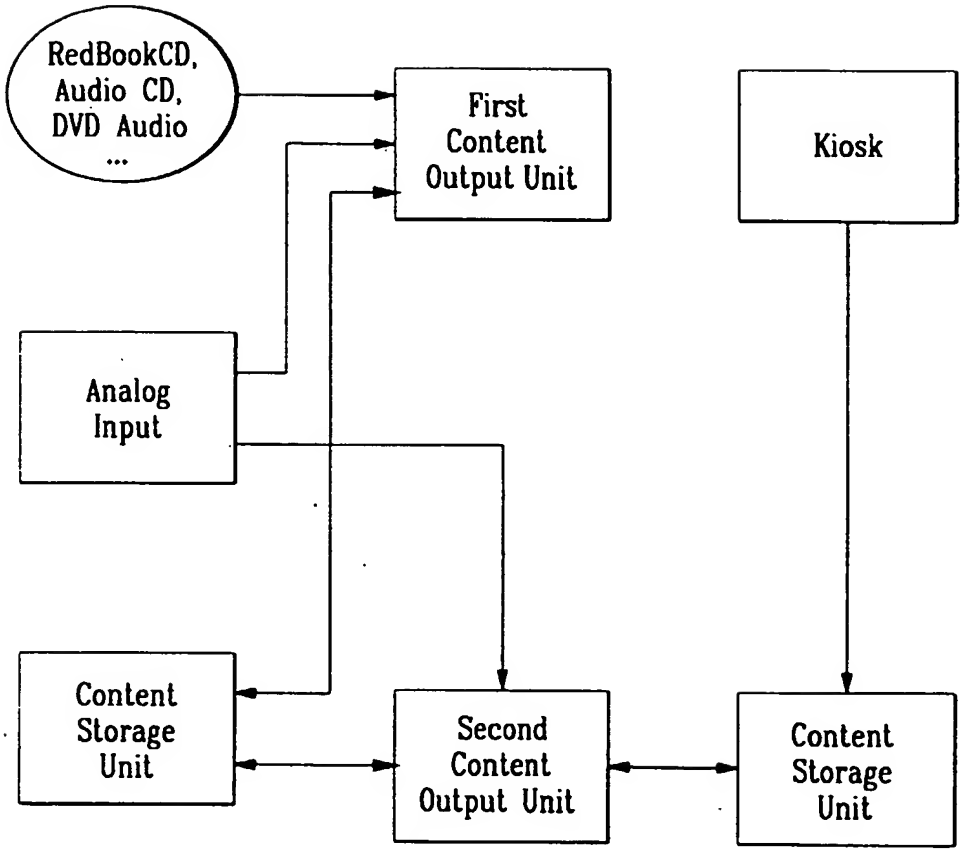
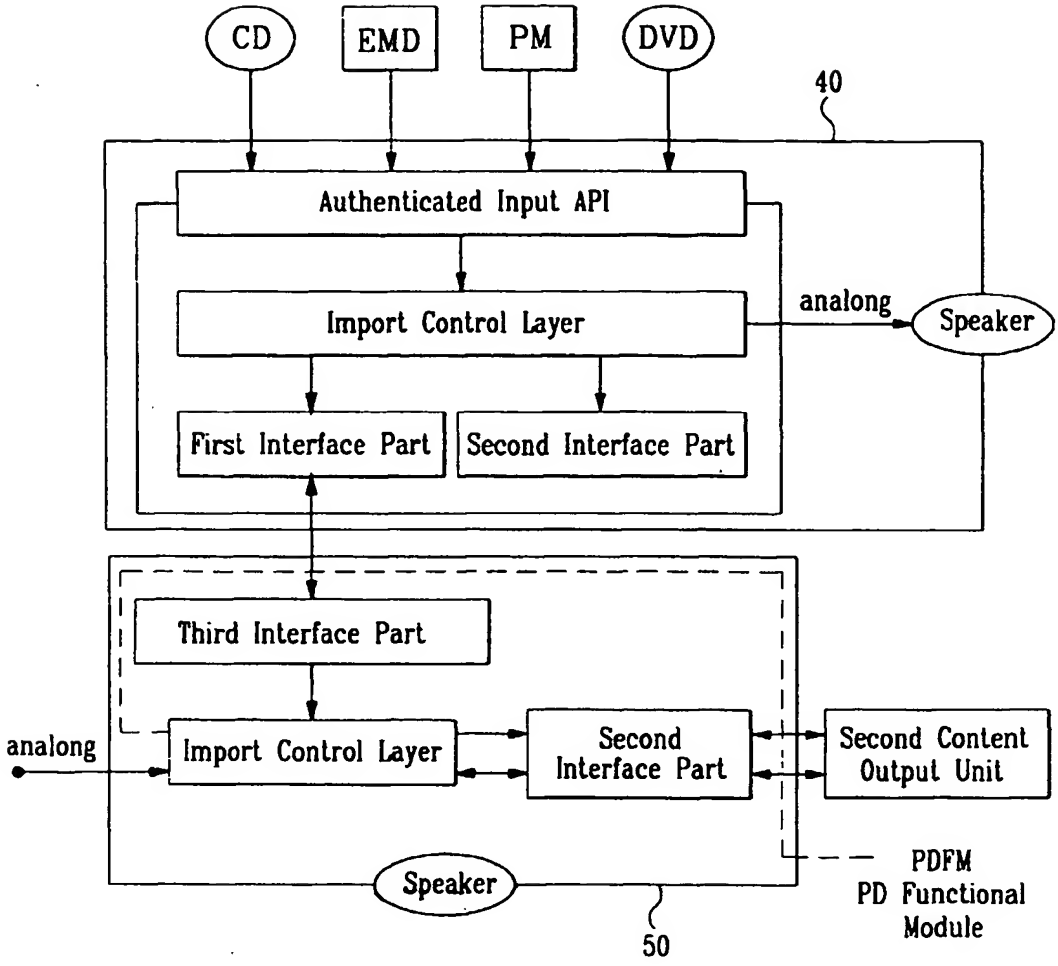

RedBookCD,
Audio CD,
DVD Audio
...
First
Content
Output Unit
Kiosk
Analog
Input
Content
Storage
Unit
Second
Content
Output Unit
Content
Storage
Unit

FIG. 9


CD
EMD
PM
DVD
40
Authenticated Input API
Import Control Layer
analong
Speaker
First Interface Part
Second Interface Part
Third Interface Part
analong
Import Control Layer
Second Interface Part
Second Content Output Unit
PDFM
PD Functional Module
Speaker
50